IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	**)**	
Defendant	**)**	

DEFENDANT'S RESPONSE TO GOOGLE'S MOTION TO FILE AMICUS CURIAE BRIEF IN SUPPORT OF NEITHER PARTY

Okello Chatrie, through counsel, responds as follows to Google's motion to file an *amicus* brief in support of neither party:

INTRODUCTION

On December 20, 2019, Google moved this Court to file an *amicus* brief in support of neither party, ECF No. 59, and included its proposed 24-page brief as an attachment. ECF No. 59-1. Mr. Chatrie recognizes Google's interest in this case and appreciates the additional context that Google presents in its brief. Most of the new information that Google proffers strongly supports Mr. Chatrie's motion to suppress evidence obtained from a "geofence" general warrant, *see* ECF No. 29, including the limitless breadth of the search involved and Google's handling of Location History information as communications content akin to a "virtual journal." *Id.* at 6.

Nonetheless, Google seeks to bolster the degree of voluntariness involved in keeping such a journal, giving the misleading impression that such data collection is always, or even generally, informed and intentional. Furthermore, the information Google has provided is incomplete. The defense has requested in discovery information on the categories of data Google collected, stored, and provided to law enforcement, as well as the specific inputs and algorithms used to produce the

responsive Location History data in this case. Google addresses some but not all of these issues in its brief, seeming to pick and choose what it wishes to address.

Consequently, Mr. Chatrie must object to the Court's consideration of Google's brief without further opportunity to obtain discovery from Google and examine Google representatives capable of providing answers to the legal and factual questions raised by their brief. A thorough understanding and examination of the technology at issue here is essential to the full and fair resolution of the significant constitutional issues raised by this case. Google has already demonstrated its willingness to participate in these proceedings. This Court should require its future participation as necessary to assess to the accuracy of the new facts it seeks to interject, or alternatively, to reconsider the motion to participate as *amicus*.

ARGUMENT

I. Google's Brief Supports Mr. Chatrie's General Warrant & Search Arguments

Google distinguishes the geofence warrant at issue here from other types of law enforcement requests, emphasizing that it requires a uniquely broad search of all Google users' timelines. *See* ECF No. 59-1 at 11. Whereas typical requests compel Google to disclose information associated with a specific user, "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." *Id*. Even so-called "tower dumps" are more limited in scope than geofence warrants. As Google explains, a tower dump "requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time." *Id*. at 14. As a result, the number of people directly affected by a tower dump has an upper limit, *i.e.*, the number of devices actually present in the area. By contrast, a geofence search has no such cap because "Google has no way to identify which of its users were present in the area of interest without searching the [location history] information

stored by every Google user." *Id*. In other words, the initial stage of *any* geofence warrant necessarily entails searching *every* user for whom Google has location history data.

Google's explanation of the search process supports Mr. Chatrie's argument that geofence warrants are unconstitutional general warrants. As Mr. Chatrie contends, geofence warrants are overbroad and lack particularity because they "authorize the search of an unlimited number of people's location data," ECF No. 48 at 4, rendering them unconstitutional from the outset. *See also* ECF No. 29 at 16-24. Regardless of how many devices Google initially identifies—be it 9, 19, or 9,000—the process of doing so is the same: "Google must search across all [Location History] journal entries to identify users with potentially responsive [Location History] data, and then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." ECF No. 59-1 at 12-13. There is no probable cause to justify such a boundless search, and the discretion it affords to both Google and the government demonstrates a profound lack of particularity. Such a warrant is no warrant at all, but an unconstitutional general warrant. *See* ECF No. 29 at 17-21.

Google's description of Location History information as a personal "journal" further reinforces this conclusion. *See* ECF No. 59-1 at 6. Google states that Location History information is not a "business record" in any traditional sense, but "is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels." *Id*. Thus, from Google's perspective, it is akin to email stored on Google's Gmail service or personal documents stored remotely on Google Drive. *Id.* at 9, 17. Google asserts that it "is stored with Google primarily for the user's own use and benefit," *id.* at 9, and as a result, treats it as communications "contents" for purposes of the Stored Communications Act. *Id.* at 16-17.

In this light, Google functions as a trusted bailee of location history information that is created by and belongs to individual Google users. Thus, as Mr. Chatrie contends, his location information is his personal property—his own papers and effects—even though Google may be responsible for collecting and maintaining it. *See* ECF No. 29 at 15; *see also Ex parte Jackson*, 96 U.S. 727, 733 (1878) (finding a Fourth Amendment interest letters entrusted to mail carriers). Google, in turn, owes a duty to Mr. Chatrie to keep his location data safe and not disclose it to others. *See, e.g.*, 18 U.S.C. § 2702(a)(1) and (2) (prohibiting service providers from voluntarily divulging the contents of communications); Google, Privacy Policy (Dec. 19, 2019), https://policies.google.com/privacy?hl=en-US#infosharing (describing the limited circumstances in which Google will disclose user data). As Justice Gorsuch recognized in *Carpenter v. United States*, the Fourth Amendment protects one's papers and effects that are held by a third party through such a bailment. 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) ("Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest."). Likewise, Justices Kennedy, Thomas, and Alito all acknowledged that the third-party doctrine should not apply where businesses are the bailees or custodians of records with a duty to hold them for a defendant's use. *Id.* at 2228, 2230 (Kennedy, J., dissenting).

By compelling Google to turn over Mr. Chatrie's location history, the government infringed on his property interest in that data. Such a trespass constitutes a Fourth Amendment search and seizure, just as surely as if the government had searched and seized papers in Mr. Chatrie's hotel room or safety deposit box. *See Stoner v. California*, 376 U.S. 483, 490 (1964) ("[A] guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures."); *Couch v. United States*, 409 U.S. 322, 337 (1973) (Brennan, J., concurring)

(suggesting that individuals have a reasonable expectation of privacy in the contexts of a safety deposit box).

In this case, however, the government went even further. The geofence warrant here is the digital equivalent of searching every safety deposit box in every branch of a global bank to find one piece of stolen property. Yet any warrant purporting to authorize such a search would be an impermissible general warrant, void as a basic principle of both English common law and the Fourth Amendment. *See, e.g.*, William Hawkins, 2 *A Treatise of the Pleas of the Crown* 84 (Professional Books 1973) (P.R. Glazebrook, ed) ("I do not find any good Authority, That a Justice can justify sending a general Warrant to search all suspected Houses in general for stolen Goods, because such Warrant seems to be illegal in the very Face of it"); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a warrant to search all suspected places, stores, shops and barns in town for stolen goods was an unlawful general warrant). The same principle applies here. Google's analogy to personal journals simply underscores the property rights affected by a geofence request and highlights the impermissibility of a general warrant authorizing the search of all such data.

II. Enabling Location History Does Not Defeat Mr. Chatrie's Expectation of Privacy in His Data

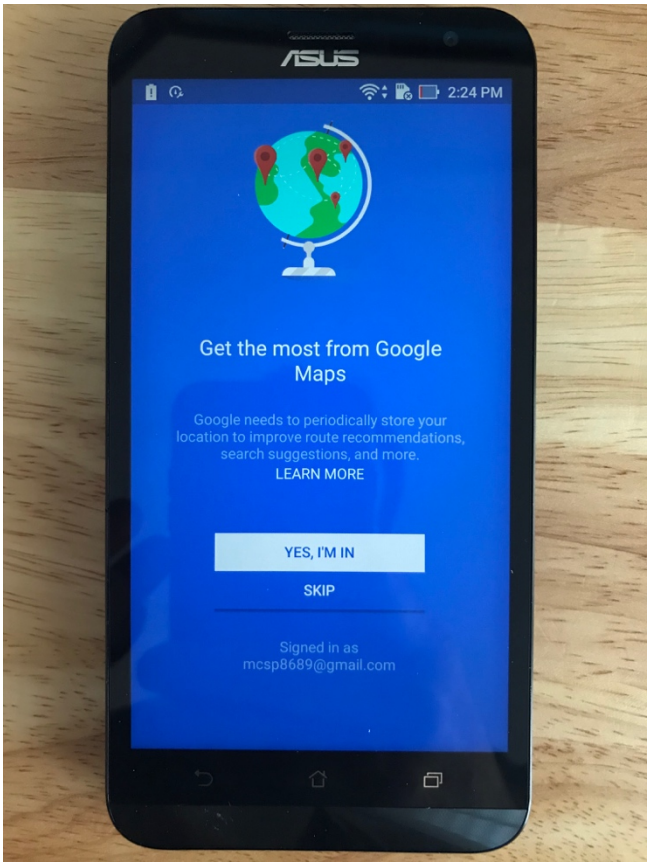
Although Mr. Chatrie appreciates Google's comparison of Location History information to a personal journal, it is not at all clear that it is a journal most people intend to keep. Google points to the account settings users must enable for the Location History service to function, claiming that the defense "errs in asserting that '[i]ndividuals do not voluntarily share their location information with Google,' . . . and that the acquisition of user location records by Google is 'automatic and inescapable.'" ECF No. 59-1 at 9. But in practice, the process for enabling Location History is not nearly as deliberate or informed as Google's brief may lead one to believe.

Google states that Location History will function only when a user takes multiple affirmative steps to enable it. According to Google, a user must (1) opt into Location History as a setting; (2) enable the "Location Reporting" feature; (3) enable the device-location setting; (4) permit location sharing with Google; (5) power on the device and sign into Google; and (6) travel with the device. *Id.* at 8. Yet virtually all of these steps may be accomplished in the first few moments of setting up and using a new device, such as the Samsung Galaxy S9 used by Mr. Chatrie, while the full consequences of doing so would not be apparent the ordinary user.

The Samsung Galaxy S9 is a mobile device that uses Google's Android operating system. As a result, one of the very first steps in setting up an S9 is to log into or create a Google account, the prompts for which appear prior to even creating a passcode for the device. *See, e.g.*, Tech ARP, *Setting Up The Samsung Galaxy S9 For The First Time*, YouTube (Mar. 8, 2018), https://www.youtube.com/watch?v=n-giid2lc_4. While it is possible to skip this step, attempting to do so yields a pop-up warning from Google that doing so will prevent the user from: downloading apps, music, and games; syncing services like Calendar and Contacts; or activating "device protection" features. *Id*. In short, most of the features commonly associated with a modern mobile device, apart from voice calls and web browsing, would be unavailable to an ordinary user who does not log into a Google account. As a result, requirement (5) is quickly satisfied without any reference to Location History. Moreover, the S9 comes out of the box with the device-location setting enabled, satisfying requirement (3). Disabling this setting renders the device incapable of many basic functions.

Requirements (1), (2), and (4) are likely to occur simultaneously when opening an application like Google Maps for the first time. When setting up an Android device similar to the S9, the defense immediately encountered a full screen from Google prompting the user to "Get the most from Google Maps," which states only that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." A button reading "YES I'M IN" is highlighted while options to "SKIP" and "LEARN MORE" were not.

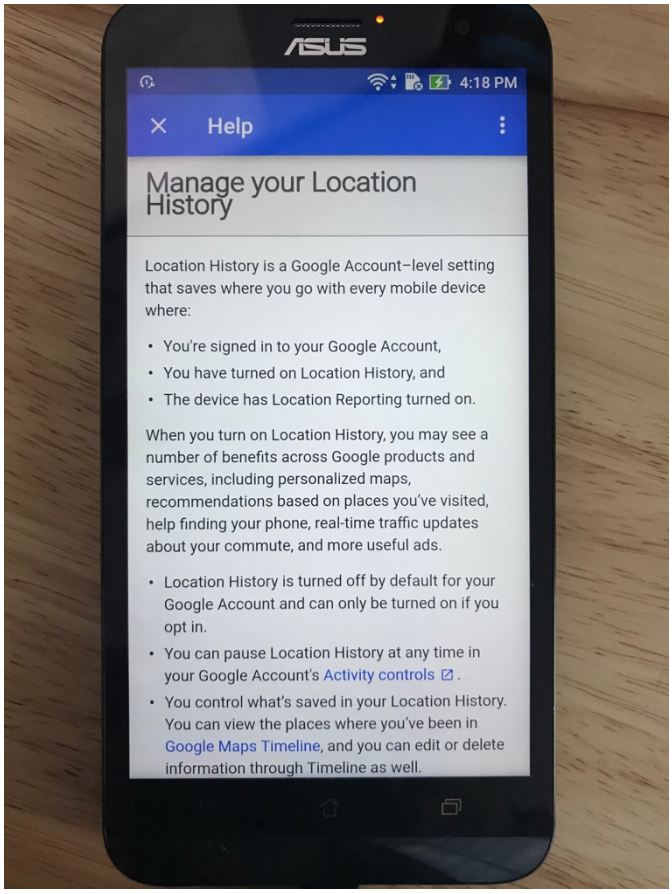
Figure 1



Clicking "YES I'M IN" enabled Location History and turned on Location Reporting, apparently satisfying both requirements (1) and (2), despite the fact that neither Location History nor Location Reporting are mentioned by name. The "LEARN MORE" section informs users that their location information will be reported to Google by enabling Location History, presumably satisfying requirement (4) at the same time. Significantly, there appears to be no way to enable Location History without also enabling Location Reporting and permitting location sharing with Google. In short, requirements (1), (2), and (4) are not independent requirements, but part and parcel of a single click. Consequently, after just the first few minutes on a new Android device like the S9, most users will have accomplished steps (1)-(5)—simply by setting it up, opening Maps, and following Google's prompts. All that remains is to move around in order to satisfy requirement (6).

Critically, the full consequences of taking these initial steps is likely not apparent to the ordinary user. There is nothing in the on-screen prompts to indicate that tapping "YES, I'M IN" will start a log of every step a user takes and share it with Google. It does not mention Location History or Location Reporting explicitly. And while the "LEARN MORE" section mentions "Google Maps Timeline" as a way to "view the places where you've been," it does not elaborate. Instead, Google takes that opportunity to explain why users should enable Location History, stating: "When you turn on Location History, you may see a number of benefits across Google products and services, including personalized maps, recommendations based on places you've visited, help finding your phone, real-time traffic updates about your commute, and more useful ads." When presented with the option in this fashion, it is easy to see how users may enable Location History without realizing the full implications of their decision.

Figure 2



Consequently, Google's description of the opt-in process for Location History does not accurately reflect the user experience, making it appear as if the decision is more intentional and informed than it really is. This raises significant doubt about the degree to which enabling Location History is truly informed and voluntary, as Google's six requirements may be quickly and easily satisfied without any mention of Location History or Location Reporting. Rather, ordinary users

like Mr. Chatrie are very likely to be unaware that Location History is on. Even computer security experts have reported not realizing that the feature had been enabled. *See, e.g.*, Matt Boddy, *The Google tracking feature you didn't know you'd switched on*, Naked Security (Oct. 3, 2017), https://nakedsecurity.sophos.com/2017/10/03/the-google-tracking-feature-you-didnt-know-youd-switched-on/. In this sense, Location History is effectively "inescapable and automatic" for ordinary Google users.

Even if enabling Location History requires a weak affirmative step, Mr. Chatrie still maintains a reasonable expectation of privacy in his data. All cell phone users, for example, must agree to share their cell site location information with the phone company, pursuant to the company's terms of service and as required for the phone to function. But doing so does not waive their Fourth Amendment protection in that data, as the intended scope of that sharing is limited accordingly. As the Florida Supreme Court recognized in *Tracey v. State*, conveying personal information to a third party for personal purposes cannot be considered disclosure for all purposes, especially to parties who were not involved in the transaction. 152 So. 3d 504, 522 (Fla. 2014). Simply because a user knows that the service provider detects his location "for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes." *Id.*; *see also Carpenter*, 138 S. Ct. at 2219 (citing *Riley v. California*, 573 U.S. 373, 392 (2014)). Consequently, Mr. Chatrie had an expectation of privacy in his Location History information that he did not forfeit by conveying it to Google for his personal use.

Finally, Google asserts that it disclosed only an "anonymized" list of user accounts in steps one and two of the geofence warrant process. *See* ECF No. 59-1 at 12-13. But as Mr. Chatrie

argues, "[t]he fact that Google masks the true "Device ID" with a pseudonym does not make the data anonymous." *See* ECF No. 68 at 3. Precise geolocation information is "inherently identifiable," capable of revealing "each person's unique path through life." *Id.*; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010) (compiling computer science research showing that it is possible to "reidentify" or "deanonymize" individuals from ostensibly anonymous data). As a result, the Court should not discount the intrusiveness of the initial data returns disclosed by Google. Had the government obtained the contents of user emails but asked Google to redact the to/from information, there would be no doubt that a search had still occurred. The same holds true for geolocation information.

III. Google's Brief Raises More Questions Than It Answers, Requiring Further Discovery from Google

In moving this Court to participate as *amicus*, Google acknowledges that it is no mere observer. Instead, because of its role in executing the geofence warrant, Google recognizes that it is "well situated to explain the nature of the data and the steps Google takes in response to geofence warrants like the one at issue here." ECF No. 59-1 at 2. In fact, as Mr. Chatrie argues in support of further discovery, Google functioned as "a private actor participating in a specific criminal investigation at the behest of the government." ECF. No. 49 at 2. And as a result, the defense maintains that Google's direct and central role in the search and seizure of Mr. Chatrie's data has made it a part of the investigative team and subject to discovery. *Id*. at 2-3.

By participating as *amicus*, however, Google seeks to pick and choose which information to disclose. Some of the information in Google's brief is responsive to Mr. Chatrie's discovery request. *See* ECF No. 28. But at the same time, some answers are conspicuously absent. Mr.

Chatrie therefore requests that the Court order Google to provide further discovery to the defense or else reconsider its order granting Google's motion to participate as *amicus*.

Clear answers to Mr. Chatrie's discovery requests are material to his defense because "there is a reasonable probability" that if they are "disclosed to the defense, the result of the proceeding [will be] different." *See United States v. Bagley*, 473 U.S. 667, 682 (1985). Under Rule 16, each are material because "there is a strong indication" that each "will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *See United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010).

A. Sensorvault, Location Services, and Web & App Activity

Two sets of unresolved factual issues about Google's response to the geofence warrant remain unanswered by Google's brief. The first set concerns what categories of data Google collected, stored, and then provided to law enforcement. Mr. Chatrie requested "[d]etails concerning Google's Sensorvault," such as "how the location data is captured and collected," "how often Google collects location data" on Android and non-Android phones, and "how many individuals' tracking information is in the Sensorvault." ECF No. 28 at 2-3. He also requested information on any "data that Google initially determined to be potentially responsive to the warrant" but ultimately excluded." *See id*. at 4. However, Google's brief did not mention Sensorvault or the other categories of location information it collects, such as Web & App Activity. ECF No. 59-1. These facts are material because they illustrate Google's cooperation with law enforcement and speak to the geofence warrant's overbreadth and lack of particularity and probable cause.

Google collects location data from users through several mechanisms, of which Location History is only one—Web & App Activity, for example, is a separate category of location data, as

is Google Location Services. ECF No. 28 at 4-5; ECF No. 48 at 6-7. The geofence warrant required Google to turn over "[d]ata" on "each type of Google account that is associated with a device that was inside the geographical area" described in the warrant. ECF No. 54-1 at 4, 9. The warrant did not limit its reach to Location History information. But Google did, apparently. Google proffers that it limited step one of the search to Location History data, meaning that it did not include location data generated by Web & App Activity or other sources, contrary to the plain language of the geofence warrant. *See* ECF No. 59-1 at 12 ("In practice, although the legal requests do not necessarily reflect this limitation, such requests can only cover Google users who had LH enabled and were using it at the time in question.").

Google, however, provides no support for this assertion or rationale for why it would restrict its search to Location History data, as opposed to including Web & App Activity or Google Location Services. Instead, Google seems to be admitting that it did not fully respond to the warrant based on some sort of internal protocol. In discovery, Mr. Chatrie has requested all such policies, guidelines, and protocols, *see* ECF No. 28 at 2. In fact, Mr. Chatrie specifically requested: "Any and all Sensorvault data that Google initially determined to be potentially responsive to the warrant … but excluded from the Sensorvault data ultimately Google provided to law enforcement officials in this case, including the reason(s) for the exclusion." *Id.* at 4. The defense needs to know, for example, the extent to which this protocol was developed in conjunction with law enforcement. Information indicating that Google worked with law enforcement officials to develop this protocol would support Mr. Chatrie's argument that the geofence warrant granted too much discretion to non-judicial officers in violation of the Fourth Amendment's particularity requirement. *See* ECF No. 29 at 17-24. It also bears on Mr. Chatrie's assertion that Google was functioning as part of the prosecution team. *See* ECF No. 49 at 2-5.

At the same time, Mr. Chatrie should not be required to simply accept Google's unsupported assertion that the geofence warrant searched only Location History information. It is clear that Google collects other types of location information via Web & App Activity and Google Location Services, and the warrant appears to request all of it. But these other functions require even less informed opt-in than Location History, operating even when Location History has been disabled. *See* ECF No. 48 at 7 (Location History "is an opt-in feature but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity."). Indeed, the lack of informed consent to such data collection has been the subject of civil lawsuits in the United States and Australia.[1] Consequently, any location data shared through Web & App Activity or Google Location Services may be even less voluntary than the data obtained through Location History, further supporting Mr. Chatrie's Fourth Amendment arguments.

Similarly, the defense understands that Google maintains all three forms of location information in its "Sensorvault" database. *See* ECF Nos. 28 & 38; H. Comm. on Energy and Commerce, 116th Cong., Letter to Sundar Pichai (Apr. 23, 2019); Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. Times (Apr.

[1] While the merits of these civil lawsuits are not relevant to Mr. Chatrie's motions in this criminal case, both acknowledged the difference between Location History and Web & App Activity. The Northern District of California discussed how "turning 'off' Location History" does not mean "the places you go are no longer stored" by Web & App Activity. *See* Order Granting Defendant's Motion to Dismiss at 2, *In Re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019). "[T]urning 'off' Location History only prevented general location tracking." *Id*. By contrast, the Web & App Activity setting is "'on' by default and saves certain information about a user's 'activity on Google sites and apps.'" *Id*. In short, "the two settings are distinct." *Id*. *See also* Concise Statement at 9, NSD1760/2019, *Australian Competition and Consumer Comm'n. v. Google Australia* (N.S.W. Oct. 29, 2019) (alleging that "where Users had Location History turned 'off' (or 'paused') and the Web & App Activity setting turned 'on' . . . Google obtained and retained Personal Data about the User's location.").

13, 2019); Kate Cox, *Feds Reap Data From 1,500 Phones in Largest Reported Reverse-Location Warrant*, Ars Technica (Dec. 13, 2019), https://arstechnica.com/tech-policy/2019/12/feds-reap-data-from-1500-phones-in-largest-reported-reverse-location-warrant/. Google, however, does not mention Sensorvault or explain how it might segregate Location History data in order to conduct a geofence according to its protocol. Further discovery about the Sensorvault system—such as Google's own description of it, the system's access control and maintenance policies, and how much of which kind of data it contains—is therefore highly relevant and material to Mr. Chatrie's suppression argument. Indeed, the government's case for probable cause relies on statistics citing the number of Android and non-Android users that have their location data stored with Google. ECF No. 41 at 3-4. Mr. Chatrie therefore deserves an opportunity to verify these claims with Google.

B. Wi-Fi Access Point Locations and Google's Algorithms

The second set of unresolved factual issues concerns the inputs and algorithms used to produce the Location History data provided to law enforcement. Mr. Chatrie requested the "location/source" of the "WiFi access points for individuals' location tracking data," ECF No. 28 at 1, which Google did not provide. He also requested the "algorithms used in analyzing and storing the location data," and "all information about the accuracy of the location data," which Google did not provide. *Id*. at 1-3. This information is material because it speaks to the geofence warrant's overbreadth and lack of particularity.[2]

Most significantly, Google appears to have included devices in the step one warrant returns that were actually outside the 150-meter radius authorized by the geofence warrant. In this case,

[2] This information would also help to evaluate the accuracy of the location data, which may become relevant at a later stage in these proceedings. The raw data shows that the margin of error tends to be quite large for the data points based on Wi-Fi. *See* ECF No. 68 Ex. A.

multiple users appear to have been ensnared in the geofence as a result of driving close to, but outside of the 150-meter radius. If true, this fact would strengthen Mr. Chatrie's argument that the warrant was overbroad and lacked particularity. Indeed, that is why the defense requested discovery concerning the location of Wi-Fi access points known to Google, as well as the algorithm Google used to determine which devices were inside the radius and responsive to the warrant.

To wit, Google's brief contains multiple statements that the data points are "probabilistic estimates" with "a margin of error" and include not just a "set of coordinates" but "a value . . . that reflects Google's confidence in the reported coordinates." *See* ECF No. 59-1 at 10, *Id*. n.7, 13 n.8, 20 n.12. Google does not, however, explain how these estimates, margins of error, or confidence values are calculated. It does, however, recognize that these estimates may include "false positives – that is, that [they] will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." *See* ECF No. 59-1 at 20 n.12.

The most likely explanation for these false positives has to do with the location of the Wi-Fi access points used to determine device locations. *See* ECF No. 49 at 7. "A Wi-Fi access point can be a router, switch, Ethernet cable hub, or some other device that creates a wireless local area network." *Id*. The raw data shows that some of the location data points were based on Wi-Fi but it does not provide the location of the access points themselves. ECF No. 68 Ex. A. This is significant because when locating users, Google's algorithm appears to assume that any device connected to an access point within the 150-meter radius is also located within that radius, equating the location of the access point with the location of the device remotely connected to it. This is a false assumption. A Wi-Fi access point within the radius has its own range, which may extend well beyond the 150-meter radius. *See* Bradley Mitchell, *What Is the Range of a Typical WiFi Network?*, Lifewire (Oct. 28, 2019), https://www.lifewire.com/range-of-typical-wifi-network-816564 (last

visited Jan. 9, 2020) (stating that Wi-Fi networks have an average outdoor range of 300 feet). As a result, devices connected to such a network may be falsely included in the warrant returns even though they were physically outside the geofence.

Even with inputs that Google proffers are "highly reliable in context," Google acknowledges that its algorithm may allow for a large margin of error when locating a user. *See* ECF No. 59-1 at 20 n.12. The resulting location information may still be "sufficiently precise and reliable for the purposes for which [Location History] was designed" (*i.e.*, the commercial context), but not necessarily "for purposes for which the [Location History] service was not designed" (*i.e.*, the law enforcement context). *See* ECF No. 59-1 at 10-11 n.7, 20 n.12; Andrea M. Rodriguez, et al., *Google Timeline Accuracy Assessment and Error Prediction*, 3 Forensic Sci. Res. 240, 245 (2018) (conducting experiment and finding that Google's estimated locations with margins of error have a hit ratio of 52% when using GPS and 7% when using Wi-Fi). Such inaccuracy is not just a trial issue. As Google acknowledges, it makes "the potential incursion on privacy is quite significant indeed." *See* ECF No. 59-1 at 20 n.12.

The only way to evaluate this impact is to look at the specific inputs, including the Wi-Fi access point locations, and the algorithm responsible for determining user location based on them. This information is directly relevant to Mr. Chatrie's overbreadth and particularity arguments, as it would likely show how people outside the 150-meter radius were swept into the geofence.

CONCLUSION

Google's brief supports Mr. Chatrie's argument that the geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, requiring suppression the search results and all fruits thereof. But because Google effectively served as a member of the investigative team in this case, and because its brief does

not fully respond to Mr. Chatrie's discovery requests, the defense requests that the Court order Google to provide further discovery to the defense or else reconsider its order granting Google's motion to participate as *amicus*.

Respectfully submitted,

OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on January 10, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org